Foundation of Cryptography (0368-4162-01), Lecture 8

Encryption Schemes

Iftach Haitner, Tel Aviv University

January 3 – 17, 2012

Section 1

Definitions

Correctness

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathsf{E}, \mathsf{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathsf{E}(e, m)$ outputs a string in $c \in \{0,1\}^*$
3. $\mathsf{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathsf{D}(d, \mathsf{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

Correctness

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathrm{E}, \mathrm{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathrm{E}(e, m)$ outputs a string in $c \in \{0,1\}^*$
3. $\mathrm{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathrm{D}(d, \mathrm{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

Correctness

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathrm{E}, \mathrm{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathrm{E}(e, m)$ outputs a string in $c \in \{0,1\}^*$
3. $\mathrm{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathrm{D}(d, \mathrm{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c = \mathrm{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,

Correctness

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathrm{E}, \mathrm{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathrm{E}(e, m)$ outputs a string in $c \in \{0,1\}^*$
3. $\mathrm{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathrm{D}(d, \mathrm{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c = \mathrm{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,

- public/private key

Security

- What would we like to achieve?

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{G(1^n)_1}(m)) \equiv (m, U_{\ell(|m|)})$$

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{G(1^n)_1}(m)) \equiv (m, U_{\ell(|m|)})$$

  - Shannon – only for m with $|m| \leq |G(1^n)_1|$

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{G(1^n)_1}(m)) \equiv (m, U_{\ell(|m|)})$$

  - Shannon – only for m with $|m| \leq |G(1^n)_1|$
  - Other concerns, e.g., multiple encryptions, active adversary

Semantic Security

1. Ciphertext reveal “no information" about the plaintext

Semantic Security

1. Ciphertext reveal “no information" about the plaintext
2. Formulate via the simulation paradigm

Semantic Security

1. Ciphertext reveal “no information" about the plaintext
2. Formulate via the simulation paradigm
3. Cannot hide the message length

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A$'$ s.t. $\forall$ poly-bounded dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-bounded functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m\leftarrow\mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)]\Big| = \mathrm{neg}(n)$$

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A$'$ s.t. $\forall$ poly-bounded dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n \in \mathbb{N}}$ and poly-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathrm{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m \leftarrow \mathcal{M}_n}[\mathrm{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)]\Big| = \mathrm{neg}(n)$$

- poly-bounded?

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A$'$ s.t. $\forall$ poly-bounded dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-bounded functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathrm{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \\ -\Pr_{m\leftarrow\mathcal{M}_n}[\mathrm{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)]\Big| = \mathrm{neg}(n)$$

- poly-bounded? for simplicity we assume polynomial length

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A' s.t. $\forall$ poly-bounded dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m\leftarrow\mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)]\Big| = \operatorname{neg}(n)$$

- poly-bounded? for simplicity we assume polynomial length
- 1^n and $1^{|m|}$ can be omitted

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A′ s.t. $\forall$ poly-bounded dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-bounded functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathrm{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \\ -\Pr_{m\leftarrow\mathcal{M}_n}[\mathrm{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)]\Big| = \mathrm{neg}(n)$$

- poly-bounded? for simplicity we assume polynomial length
- 1^n and $1^{|m|}$ can be omitted
- Non-uniform definition

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A$'$ s.t. $\forall$ poly-bounded dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-bounded functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \\ -\Pr_{m\leftarrow\mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)]\Big| = \operatorname{neg}(n)$$

- poly-bounded? for simplicity we assume polynomial length
- 1^n and $1^{|m|}$ can be omitted
- Non-uniform definition
- Reflection to $\mathcal{ZK}$

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A$'$ s.t. $\forall$ poly-bounded dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n \in \mathbb{N}}$ and poly-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m \leftarrow \mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| = \operatorname{neg}(n)$$

- poly-bounded? for simplicity we assume polynomial length
- 1^n and $1^{|m|}$ can be omitted
- Non-uniform definition
- Reflection to ZK
- public-key variant – A gets e

Indistinguishablity of encryptions

- The encryption of two strings is indistinguishable

Indistinguishablity of encryptions

- The encryption of two strings is indistinguishable
- Less intuitive than semantic security, but easier to work with

Indistinguishablity of encryptions – private-key model

Definition 3 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions in the private-key model, if for any $p, \ell \in \mathrm{poly}$, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and poly-time B,

$$\left|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1]\right| = \mathrm{neg}(n)$$

Indistinguishablity of encryptions – private-key model

Definition 3 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions in the private-key model, if for any $p, \ell \in \mathrm{poly}$, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and poly-time B,

$$\left|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1]\right| = \mathrm{neg}(n)$$

- Non-uniform definition

Indistinguishablity of encryptions – private-key model

Definition 3 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions in the private-key model, if for any $p, \ell \in$ poly, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and poly-time B,

$$\left|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1]\right| = \mathrm{neg}(n)$$

- Non-uniform definition
- Public-key variant

Equivalence of definitions

Theorem 4

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ *is semantically secure iff is has indistinguishable encryptions.*

Equivalence of definitions

Theorem 4

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ is semantically secure iff is has indistinguishable encryptions.

We prove the private key case

Indistinguishablity $\Longrightarrow$ Semantic Security

Indistinguishablity $\implies$ Semantic Security

Fix $\mathcal{M}$, A, f and h, be as in Definition **??**.

Indistinguishablity $\Longrightarrow$ Semantic Security

Fix $\mathcal{M}$, A, f and h, be as in Definition **??**. We construct A$'$ as

Algorithm 5 (A$'$)

Input: 1^n, $1^{|m|}$ and $h(m)$

1. $e \leftarrow G(1^n)_1$
2. $c = E_e(1^{|m|})$
3. Output A$(1^n, 1^{|m|}, h(m), c)$

Indistinguishablity $\Longrightarrow$ Semantic Security

Fix $\mathcal{M}$, A, f and h, be as in Definition **??**. We construct A′ as

Algorithm 5 (A′)

Input: 1^n, $1^{|m|}$ and $h(m)$

1. $e \leftarrow G(1^n)_1$
2. $c = E_e(1^{|m|})$
3. Output $A(1^n, 1^{|m|}, h(m), c)$

Claim 6

A′ is a good simulator for A (according to Definition **??**)

Proving Claim ??

Assume exists infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in$ poly s.t. for any $n \in \mathcal{I}$:

$$\begin{aligned} \Big| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1} [\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \\ - \Pr_{m \leftarrow \mathcal{M}_n} [\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| > 1/p(n) \end{aligned} \quad (1)$$

Proving Claim ??

Assume exists infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in$ poly s.t. for any $n \in \mathcal{I}$:

$$\begin{aligned} \Big|\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \quad (1) \\ -\Pr_{m \leftarrow \mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)]\Big| > 1/p(n) \end{aligned}$$

Fix $n \in \mathcal{I}$ and let $x_n \in \operatorname{Supp}(\mathcal{M}_n)$ be a value that maximize **??.**

Proving Claim ??

Assume exists infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in$ poly s.t. for any $n \in \mathcal{I}$:

$$\Big| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \qquad (1)$$
$$- \Pr_{m \leftarrow \mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| > 1/p(n)$$

Fix $n \in \mathcal{I}$ and let $x_n \in \mathrm{Supp}(\mathcal{M}_n)$ be a value that maximize **??.** Assume exits algorithm B that contradicts the indistinguishability of the scheme with respect to $\{(x_n, y_n = 1^{|x_n|})\}_{n \in \mathbb{N}}$ and $\{z_n = (1^n, 1^{|x_n|}, h(1^n, x_n), f(1^n, x_n))\}_{n \in \mathbb{N}}$.

Proving Claim ??

Assume exists infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in$ poly s.t. for any $n \in \mathcal{I}$:

$$\begin{aligned} \Big| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathrm{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \quad (1) \\ - \Pr_{m \leftarrow \mathcal{M}_n}[\mathrm{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| > 1/p(n) \end{aligned}$$

Fix $n \in \mathcal{I}$ and let $x_n \in \mathrm{Supp}(\mathcal{M}_n)$ be a value that maximize **??.**
Assume exits algorithm B that contradicts the indistinguishability of the scheme with respect to
$\{(x_n, y_n = 1^{|x_n|})\}_{n \in \mathbb{N}}$ and
$\{z_n = (1^n, 1^{|x_n|}, h(1^n, x_n), f(1^n, x_n))\}_{n \in \mathbb{N}}$.

Algorithm 7 (B)

Input: $z_n = (1^n, 1^{|x_n|}, h(1^n, x_n), f(1^n, x_n)), c$
Output 1 iff $\mathrm{A}(1^n, 1^{|x_n|}, h(x+n), c) = f(1^n, x_n)$

Semantic Security $\Longrightarrow$ Indistinguishablity

Assume $\exists$ B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and a $\{z_n\}_{n\in\mathbb{N}}$, such that (wlog) for infinitely many n's:

$$\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)}$$

Semantic Security $\Longrightarrow$ Indistinguishablity

Assume $\exists$ B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and a $\{z_n\}_{n\in\mathbb{N}}$, such that (wlog) for infinitely many n's:

$$\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)}$$

- Let $\mathcal{M}_n$ be x_n wp $\frac{1}{2}$ and y_n otherwise.
- Let $f(1^n, x_n) = 1$, $f(1^n, y_n) = 0$ and $h(1^n, \cdot) = z_n$).
- Define $\mathrm{A}(1^n, 1^{\ell(n)}, z_n, c)$ to return $\mathrm{B}(z_n, c)$.

Semantic Security $\Longrightarrow$ Indistinguishablity

Assume $\exists$ B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and a $\{z_n\}_{n\in\mathbb{N}}$, such that (wlog) for infinitely many n's:

$$\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)}$$

- Let $\mathcal{M}_n$ be x_n wp $\frac{1}{2}$ and y_n otherwise.
- Let $f(1^n, x_n) = 1$, $f(1^n, y_n) = 0$ and $h(1^n, \cdot) = z_n$).
- Define $\mathrm{A}(1^n, 1^{\ell(n)}, z_n, c)$ to return $\mathrm{B}(z_n, c)$.

$$\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathrm{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \geq \frac{1}{2} + \frac{1}{p(n)}$$

Semantic Security $\Longrightarrow$ Indistinguishablity

Assume $\exists$ B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and a $\{z_n\}_{n\in\mathbb{N}}$, such that (wlog) for infinitely many n's:

$$\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)}$$

- Let $\mathcal{M}_n$ be x_n wp $\frac{1}{2}$ and y_n otherwise.
- Let $f(1^n, x_n) = 1$, $f(1^n, y_n) = 0$ and $h(1^n, \cdot) = z_n$).
- Define $\mathrm{A}(1^n, 1^{\ell(n)}, z_n, c)$ to return $\mathrm{B}(z_n, c)$.

$$\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathrm{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \geq \frac{1}{2} + \frac{1}{p(n)}$$

For *any* A′

$$\Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathrm{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] \leq \frac{1}{2}$$

Security Under Multiple Encryptions

Security Under Multiple Encryptions

Definition 8 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in \mathrm{poly}$,
$\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$,
$\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$ and polynomial-time B,

$$\begin{aligned} &\left|\Pr_{e \leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1]\right. \\ &\left.-\Pr_{e \leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\right| = \mathrm{neg}(n) \end{aligned}$$

Security Under Multiple Encryptions

Definition 8 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in \text{poly}$,
$\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$,
$\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\begin{aligned} &\left|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1]\right. \\ &\left.-\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\right| = \mathrm{neg}(n) \end{aligned}$$

Extensions:

- Different length messages

Security Under Multiple Encryptions

Definition 8 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in$ poly, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\left|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\right| = \mathrm{neg}(n)$$

Extensions:

- Different length messages
- Semantic security version

Security Under Multiple Encryptions

Definition 8 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in \text{poly}$, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\Big|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] \\ -\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\Big| = \text{neg}(n)$$

Extensions:

- Different length messages
- Semantic security version
- Public-key definition

Multiple Encryption in the Public-Key Model

Theorem 9

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Multiple Encryption in the Public-Key Model

Theorem 9

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Assume $(G, \mathrm{E}, \mathrm{D})$ is public-key secure for a single message and not for multiple messages with respect to B, $\{x_{1,t(n)}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$.

Multiple Encryption in the Public-Key Model

Theorem 9

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Assume $(G, \mathrm{E}, \mathrm{D})$ is public-key secure for a single message and not for multiple messages with respect to B, $\{x_{1,t(n)}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$.
It follows that for some function $i(n) \in [t(n)]$

$$\begin{aligned}&\Big|\Pr[\mathrm{B}(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), E_e(y_{n,i}) \ldots, E_e(y_{n,t(n)})) = 1]\\ &-\Pr[\mathrm{B}(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i}), E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)})) = 1]\Big|\\ &\quad > \mathrm{neg}(n)\end{aligned}$$

where in both cases $e \leftarrow G(1^n)_1$

Algorithm 10 (B′)

Input: 1^n, $z_n = (i(n), x_{1,t(n)}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)}, e\ ,c$
Return $\mathrm{B}(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))$

Algorithm 10 (B′)

Input: 1^n, $z_n = (i(n), x_{1,t(n)}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)}, e\ ,c$
Return $\mathrm{B}(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))$

B′ is critically using the public key

Multiple Encryption in the Private-Key Model

Fact 11

Assuming (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, but not *for multiple messages*

Multiple Encryption in the Private-Key Model

Fact 11

Assuming (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, but not *for multiple messages*

Proof: Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{n+1}$ be a (non-uniform) PRG, and for $i \in \mathbb{N}$ let g^i be its "iterated extension" to output of length i (see Lecture 2, Construction 15).

Multiple Encryption in the Private-Key Model

Fact 11

Assuming (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, but not *for multiple messages*

Proof: Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{n+1}$ be a (non-uniform) PRG, and for $i \in \mathbb{N}$ let g^i be its "iterated extension" to output of length i (see Lecture 2, Construction 15).

Construction 12

- $G(1^n)$ outputs $e \leftarrow \{0,1\}^n$,
- $\mathrm{E}_e(m)$ outputs $g^{|m|}(e) \oplus m$
- $\mathrm{D}_e(c)$ outputs $g^{|c|}(e) \oplus c$

Claim 13

(G, E, D) has private-key indistinguishable encryptions for a single message

Proof:

Claim 13

$(G, \mathrm{E}, \mathrm{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it.

Claim 13

$(G, \mathrm{E}, \mathrm{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Wlog,

$$\left|\Pr[\mathrm{B}(z_n, g^{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathrm{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \mathrm{neg}(n) \quad (2)$$

Claim 13

(G, E, D) has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Wlog,

$$\left|\Pr[\mathrm{B}(z_n, g^{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathrm{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \mathrm{neg}(n) \tag{2}$$

Hence, B implies a (non-uniform) distinguisher for g

Claim 13

$(G, \mathrm{E}, \mathrm{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Wlog,

$$\left|\Pr[\mathrm{B}(z_n, g^{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathrm{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \mathrm{neg}(n) \tag{2}$$

Hence, B implies a (non-uniform) distinguisher for g

Claim 14

$(G, \mathrm{E}, \mathrm{D})$ does not have a private-key indistinguishable encryptions for multiple messages

Claim 13

$(G, \mathrm{E}, \mathrm{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Wlog,

$$\left|\Pr[\mathrm{B}(z_n, g^{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathrm{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \mathrm{neg}(n) \quad (2)$$

Hence, B implies a (non-uniform) distinguisher for g

Claim 14

$(G, \mathrm{E}, \mathrm{D})$ does not have a private-key indistinguishable encryptions for multiple messages

Proof:

Claim 13

$(G, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Wlog,

$$\left|\Pr[\mathsf{B}(z_n, g^{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \operatorname{neg}(n) \tag{2}$$

Hence, B implies a (non-uniform) distinguisher for g

Claim 14

$(G, \mathsf{E}, \mathsf{D})$ does not have a private-key indistinguishable encryptions for multiple messages

Proof: Take $x_{n,1} = x_{n,2}$, $y_{n,1} \neq y_{n,2}$ and $\mathsf{D}(c_1, c_2)$ outputs 1 iff $c_1 = c_2$

Section 2

Constructions

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of a single length (here the length is n).

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of a single length (here the length is n).

Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of a single length (here the length is n).
Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Construction 15

- $G(1^n)$: output $e \leftarrow \mathcal{F}_n$,
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(r, e(r) \oplus m)$
- $\mathrm{D}_e(r,c)$: output $e(r) \oplus c$

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of a single length (here the length is n).
Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Construction 15

- $G(1^n)$: output $e \leftarrow \mathcal{F}_n$,
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(r, e(r) \oplus m)$
- $\mathrm{D}_e(r, c)$: output $e(r) \oplus c$

Claim 16

$(G, \mathrm{E}, \mathrm{D})$ has private-key indistinguishable encryptions for a multiple messages

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of a single length (here the length is n).

Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Construction 15

- $G(1^n)$: output $e \leftarrow \mathcal{F}_n$,
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(r, e(r) \oplus m)$
- $\mathrm{D}_e(r,c)$: output $e(r) \oplus c$

Claim 16

$(G, \mathrm{E}, \mathrm{D})$ has private-key indistinguishable encryptions for a multiple messages

Proof:

Public key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) family of trapdoor permutations (see Lecture 6, Def 8) and let b be an hardcore predicate for f.

Public key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) family of trapdoor permutations (see Lecture 6, Def 8) and let b be an hardcore predicate for f.

Construction 17 (bit encryption)

- $G(1^n)$: output $(e, d) \leftarrow G(1^n)$
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0, 1\}^n$ and output $(y = f_e(r), c = b(r) \oplus m)$
- $\mathrm{D}_d(y, c)$: output $b(\mathrm{Inv}_d(y)) \oplus c$

Public key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) family of trapdoor permutations (see Lecture 6, Def 8) and let b be an hardcore predicate for f.

Construction 17 (bit encryption)

- $G(1^n)$: output $(e, d) \leftarrow G(1^n)$
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(y = f_e(r), c = b(r) \oplus m)$
- $\mathrm{D}_d(y, c)$: output $b(\mathrm{Inv}_d(y)) \oplus c$

Claim 18

$(G, \mathrm{E}, \mathrm{D})$ has public-key indistinguishable encryptions for a multiple messages

Public key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) family of trapdoor permutations (see Lecture 6, Def 8) and let b be an hardcore predicate for f.

Construction 17 (bit encryption)

- $G(1^n)$: output $(e, d) \leftarrow G(1^n)$
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(y = f_e(r), c = b(r) \oplus m)$
- $\mathrm{D}_d(y, c)$: output $b(\mathrm{Inv}_d(y)) \oplus c$

Claim 18

$(G, \mathrm{E}, \mathrm{D})$ has public-key indistinguishable encryptions for a multiple messages

- We believe that public-key encryptions are of different complexity than private-key ones

Section 3

Active Adversaries

Active Adversaries

- Dream version

Active Adversaries

- Dream version
- Chosen plaintext attack (CPA):
  Adversary can ask for encryptions done by the encryption key

Active Adversaries

- Dream version
- Chosen plaintext attack (CPA):
  Adversary can ask for encryptions done by the encryption key
- Passive chosen ciphertext attack (CCA1):
  same as CPA, but the adversary can for *decryptions* using the decryption key, before seeing the challenge

Active Adversaries

- Dream version
- Chosen plaintext attack (CPA):
  Adversary can ask for encryptions done by the encryption key
- Passive chosen ciphertext attack (CCA1):
  same as CPA, but the adversary can for *decryptions* using the decryption key, before seeing the challenge
- Adaptive chosen ciphertext attack (CCA2):
  same as CCA2, but the adversary can for decryptions using the decryption key *after* seeing the challenge, but not of the challenge itself

Active Adversaries

- Dream version
- Chosen plaintext attack (CPA):
  Adversary can ask for encryptions done by the encryption key
- Passive chosen ciphertext attack (CCA1):
  same as CPA, but the adversary can for *decryptions* using the decryption key, before seeing the challenge
- Adaptive chosen ciphertext attack (CCA2):
  same as CCA2, but the adversary can for decryptions using the decryption key *after* seeing the challenge, but not of the challenge itself

Active Adversaries

- Dream version
- Chosen plaintext attack (CPA):
  Adversary can ask for encryptions done by the encryption key
- Passive chosen ciphertext attack (CCA1):
  same as CPA, but the adversary can for *decryptions* using the decryption key, before seeing the challenge
- Adaptive chosen ciphertext attack (CCA2):
  same as CCA2, but the adversary can for decryptions using the decryption key *after* seeing the challenge, but not of the challenge itself

- In the public-key settings, the adversary is also given the public key

Active Adversaries

- Dream version
- Chosen plaintext attack (CPA):
  Adversary can ask for encryptions done by the encryption key
- Passive chosen ciphertext attack (CCA1):
  same as CPA, but the adversary can for *decryptions* using the decryption key, before seeing the challenge
- Adaptive chosen ciphertext attack (CCA2):
  same as CCA2, but the adversary can for decryptions using the decryption key *after* seeing the challenge, but not of the challenge itself

- In the public-key settings, the adversary is also given the public key
- We focus on indistinguishability, but each of the above definitions has an equivalent semantic security variant.

CPA Security

Let $(G, \mathsf{E}, \mathsf{D})$ be an an encryption scheme. For a pair of alg. $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$, $n \in \mathbb{N}$, $z \in \{0,1\}^*$ and $b \in \{0,1\}$, we let:

Experiment 19 ($\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z_n}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(x_0, x_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(x_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

CPA Security

Let $(G, \mathsf{E}, \mathsf{D})$ be an an encryption scheme. For a pair of alg. $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$, $n \in \mathbb{N}$, $z \in \{0,1\}^*$ and $b \in \{0,1\}$, we let:

Experiment 19 ($\mathrm{Exp}^{\mathrm{CPA}}_{\mathsf{A},n,z_n}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(x_0, x_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(x_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

Definition 20 (private key CPA)

$(G, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model under CPA attack, if $\forall$ PPT $\mathsf{A}_1, \mathsf{A}_2$, and poly-bounded $\{z_n\}_{n\in\mathbb{N}}$:

$$|\Pr[\mathrm{Exp}^{\mathrm{CPA}}_{\mathsf{A},n,z_n}(0) = 1] - \Pr[\mathrm{Exp}^{\mathrm{CPA}}_{\mathsf{A},n,z_n}(1) = 1]| = \mathrm{neg}(n)$$

- The scheme from Construction **??** has indistinguishable encryptions in the private-key model under CPA attack(for short, private-key CPA secure)

- The scheme from Construction **??** has indistinguishable encryptions in the private-key model under CPA attack(for short, private-key CPA secure)
- The scheme from Construction **??** has indistinguishable encryptions in the public-key model (for short, public-key CPA secure)

- The scheme from Construction **??** has indistinguishable encryptions in the private-key model under CPA attack(for short, private-key CPA secure)
- The scheme from Construction **??** has indistinguishable encryptions in the public-key model (for short, public-key CPA secure)
- In both cases, definitions are *not* equivalent

CCA Security

Experiment 21 ($\mathrm{Exp}^{\mathrm{CCA1}}_{\mathrm{A},n,z_n}(b)$)

1. $(e,d) \leftarrow G(1^n)$
2. $(x_0, x_1, s) \leftarrow \mathrm{A}_1^{E_e(\cdot),D_d(\cdot)}(1^n, z)$
3. $c \leftarrow \mathrm{E}_e(x_b)$
4. Output $\mathrm{A}_2^{E_e(\cdot)}(1^n, s, c)$

CCA Security

Experiment 21 ($\mathrm{Exp}^{\mathrm{CCA1}}_{\mathsf{A},n,z_n}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(x_0, x_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot),D_d(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(x_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

Experiment 22 ($\mathrm{Exp}^{\mathrm{CCA2}}_{\mathsf{A},n,z_n}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(x_0, x_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot),D_d(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(x_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot),D_d^{\neg c}(\cdot)}(1^n, s, c)$

Definition 23 (private key CCA1/CCA2)

$(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions in the private-key model under $x \in \{\mathrm{CCA1}, \mathrm{CCA2}\}$ attack, if $\forall$ PPT $\mathrm{A}_1, \mathrm{A}_2$, and poly-bounded $\{z_n\}_{n\in\mathbb{N}}$:

$$|\Pr[\mathrm{Exp}^{x}_{\mathrm{A},n,z_n}(0) = 1] - \Pr[\mathrm{Exp}^{x}_{\mathrm{A},n,z_n}(1) = 1]| = \mathrm{neg}(n)$$

Definition 23 (private key CCA1/CCA2)

$(G, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model under $x \in \{\mathrm{CCA1}, \mathrm{CCA2}\}$ attack, if $\forall$ PPT $\mathsf{A}_1, \mathsf{A}_2$, and poly-bounded $\{z_n\}_{n\in\mathbb{N}}$:

$$|\Pr[\mathrm{Exp}^x_{\mathsf{A},n,z_n}(0) = 1] - \Pr[\mathrm{Exp}^x_{\mathsf{A},n,z_n}(1) = 1]| = \mathrm{neg}(n)$$

- Public key definition is analogous

Private-key CCA2

- Is the scheme from Construction **??** private-key CCA1 secure?

Private-key CCA2

- Is the scheme from Construction **??** private-key CCA1 secure?
- Is it CCA2 secure?

Let $(G, \mathsf{E}, \mathsf{D})$ be a private key CPA scheme, and let $(\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ be an existential unforgeable MAC.

Construction 24

- $G'(1^n)$: Output $(e \leftarrow G_E(1^n), k \leftarrow \mathsf{Gen}_M(1^n))$.[a]
- $\mathsf{E}'_{d,k}(m)$: let $c = \mathsf{E}_e(m)$ and output $(c, t = \mathsf{Mac}_k(c))$
- $\mathsf{D}_{e,k}(c, t)$: if $\mathsf{Vrfy}_k(c, t) = 1$, output $\mathsf{D}_e(c)$. Otherwise, output $\perp$

[a] We assume for simplicity that the encryption and decryption keys are the same.

Private-key CCA2

- Is the scheme from Construction **??** private-key CCA1 secure?
- Is it CCA2 secure?

Let $(G, \mathsf{E}, \mathsf{D})$ be a private key CPA scheme, and let $(\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ be an existential unforgeable MAC.

Construction 24

- $G'(1^n)$: Output $(e \leftarrow G_E(1^n), k \leftarrow \mathsf{Gen}_M(1^n))$.[a]
- $\mathsf{E}'_{d,k}(m)$: let $c = \mathsf{E}_e(m)$ and output $(c, t = \mathsf{Mac}_k(c))$
- $\mathsf{D}_{e,k}(c, t)$: if $\mathsf{Vrfy}_k(c, t) = 1$, output $\mathsf{D}_e(c)$. Otherwise, output $\perp$

[a] We assume for simplicity that the encryption and decryption keys are the same.

Theorem 25

Construction **??** *is a private-key* CCA2 *secure encryption scheme.*

Theorem 25

Construction **??** *is a private-key* CCA2 *secure encryption scheme.*

Proof: ?

Public-key CCA1

Public-key CCA1

Let $(G, \mathsf{E}, \mathsf{D})$ be a public-key CPA scheme and let (P, V) be a NIZK for $\mathcal{L} = \{(c_0, c_1, pk_0, pk_1) \colon \exists (m, r_0, r_1) \ \ s.t.\ c_0 = \mathsf{E}_{pk_0}(m, r_0) \wedge c_1 = \mathsf{E}_{pk_1}(m, r_1)\}$

Construction 26 (The Naor-Yung Paradigm)

- $G'(1^n)$:
  1. For $i \in \{0, 1\}$: set $(sk_i, pk_i) \leftarrow G(1^n)$.
  2. Set $pk' = (pk_0, pk_1, r \leftarrow \{0, 1\}^{\ell(n)})$ and $sk' = (pk', sk_0, sk_1)$
- $\mathsf{E}'_{pk'}(m)$:
  1. For $i \in \{0, 1\}$: $c_i = \mathsf{E}_{pk_i}(m, c_i)$
  2. π be the proof of P that c_0 and c_1 encrypt the same message (with respect to r)
  3. Output (c_0, c_1, π).
- $\mathsf{D}'_{sk'}(c_0, c_1, \pi)$: If π is a valid proof for (c_0, c_1, pk_0, pk_1), return $\mathsf{D}_{sk_0}(c_0)$. Otherwise, return $\perp$

- We assume wlg. that the encryption key output by $G(1^n)$ is of length at least n

- We assume wlg. that the encryption key output by $G(1^n)$ is of length at least n
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using ”security parameter" n.

- We assume wlg. that the encryption key output by $G(1^n)$ is of length at least n
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using ”security parameter" n.
- Is the scheme CCA1 secure?

Public-key CCA1

- We assume wlg. that the encryption key output by $G(1^n)$ is of length at least n
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using ”security parameter" n.
- Is the scheme CCA1 secure? We need the NIZK to be “adaptive secure".

- We assume wlg. that the encryption key output by $G(1^n)$ is of length at least n
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using "security parameter" n.
- Is the scheme CCA1 secure? We need the NIZK to be "adaptive secure".

Theorem 27

Assuming that (P, V) *is adaptive-secure, then Construction* **??** *is a public-key* CCA1 *secure encryption scheme.*

- We assume wlg. that the encryption key output by $G(1^n)$ is of length at least n
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using "security parameter" n.
- Is the scheme CCA1 secure? We need the NIZK to be "adaptive secure".

Theorem 27

Assuming that (P, V) *is adaptive-secure, then Construction* **??** *is a public-key* CCA1 *secure encryption scheme.*

Proof: Given an attacker A' for the CCA1 security of $(G', \mathsf{E}', \mathsf{D}')$, we use it to construct an attacker A on the CPA security of $(G, \mathsf{E}, \mathsf{D})$.
Let $\mathsf{S} = (\mathsf{S}_1, \mathsf{S}_2)$ be the (adaptive) simulator for $(\mathsf{P}, \mathsf{V}, \mathcal{L})$

Algorithm 28 (A)

1. On $(1^n, pk)$:
   - let $j \leftarrow \{0,1\}$
   - Let $pk_{1-j} = pk$, $(pk_j, sk_j) \leftarrow G(1^n)$ and $r \leftarrow \mathrm{S}_1(1^n)$
   - Send $pk' = (pk_0, pk_1, r)$ to A′
2. On query (c_0, c_1, π) of A′ to D′: if π is a valid proof for $(c_0, c_1, pk_0, pk_1) \in \mathcal{L}$, return $\mathrm{D}_{sk_j}(c_j)$. Otherwise, return $\perp$.
3. Output the same pair (m_0, m_1) as A′ does
4. On challenge c $(= \mathrm{E}_{sk}(m_b))$:
   - Set $c_{1-j} = c$, $a \leftarrow \{0,1\}$, $c_j = \mathrm{E}_{pk_j}(m_a)$, and $\pi \leftarrow \mathrm{S}_2((c_0, c_1, pk_0, pk_1), r)$
   - Send $c' = (c_0, c_1, \pi)$ to A′
5. Output the same value that A′ does

Claim 29

Assume that A' breaks the CCA1 security of $(G', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(G, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \mathrm{neg}(n))/2$.

Claim 29

Assume that A' breaks the CCA1 security of $(G', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(G, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \mathrm{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ “makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \mathrm{neg}(n) \qquad (3)$$

Claim 29

Assume that A$'$ breaks the CCA1 security of $(G', \mathrm{E}', \mathrm{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(G, \mathrm{E}, \mathrm{D})$ with probability $(\delta(n) - \mathrm{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathrm{A}' \text{ “makes" } \mathrm{A}(1^n) \text{ decrypt an invalid cipher}] = \mathrm{neg}(n) \quad (3)$$

Ignoring negligible terms, in the following we assume that A that always encrypts using sk_0.

Claim 29

Assume that A′ breaks the CCA1 security of $(G', \mathrm{E}', \mathrm{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(G, \mathrm{E}, \mathrm{D})$ with probability $(\delta(n) - \mathrm{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathrm{A}' \text{ “makes" } \mathrm{A}(1^n) \text{ decrypt an invalid cipher}] = \mathrm{neg}(n) \qquad (3)$$

Ignoring negligible terms, in the following we assume that A that always encrypts using sk_0.
Let $\mathrm{A}'(1^n, a^*, b^*)$ be the output of $\mathrm{A}'(1^n)$ in the emulation induced by A, where $a = a^*$ and $b = b^*$.

Claim 29

Assume that A′ breaks the CCA1 security of $(G', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(G, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \mathrm{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ “makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \mathrm{neg}(n) \quad (3)$$

Ignoring negligible terms, in the following we assume that A that always encrypts using sk_0.
Let $\mathsf{A}'(1^n, a^*, b^*)$ be the output of $\mathsf{A}'(1^n)$ in the emulation induced by A, where $a = a^*$ and $b = b^*$. It holds that

1. $\mathsf{A}'(1^n, 0, 1) \equiv \mathsf{A}'(1^n, 1, 0)$

Claim 29

Assume that A' breaks the CCA1 security of $(G', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(G, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \operatorname{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ “makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \operatorname{neg}(n) \quad (3)$$

Ignoring negligible terms, in the following we assume that A that always encrypts using sk_0.
Let $\mathsf{A}'(1^n, a^*, b^*)$ be the output of $\mathsf{A}'(1^n)$ in the emulation induced by A, where $a = a^*$ and $b = b^*$. It holds that

1. $\mathsf{A}'(1^n, 0, 1) \equiv \mathsf{A}'(1^n, 1, 0)$
2. The adaptive zero-knowledge of (P, V) yields that $|\Pr[\mathsf{A}'(1^n, 1, 1) = 1] - \Pr[\mathsf{A}'(1^n, 0, 0) = 1]| \geq \delta(n) - \operatorname{neg}(n)$

Let A(b) be the outputs of A when the challenge is b.

Let A(b) be the outputs of A when the challenge is b.

$$
\begin{aligned}
&|\Pr[A(1) = 1] - \Pr[A(0) = 1]| \\
&\quad = |\frac{1}{2}(\Pr[A'(0,1) = 1] + \Pr[A'(1,1) = 1]) \\
&\qquad - \frac{1}{2}(\Pr[A'(0,0) = 1] + \Pr[A'(1,0) = 1])|
\end{aligned}
$$

Let A(b) be the outputs of A when the challenge is b.

$$
\begin{aligned}
&|\Pr[A(1) = 1] - \Pr[A(0) = 1]| \\
&\quad = |\frac{1}{2}(\Pr[A'(0,1) = 1] + \Pr[A'(1,1) = 1]) \\
&\qquad -\frac{1}{2}(\Pr[A'(0,0) = 1] + \Pr[A'(1,0) = 1])| \\
&\quad \geq \frac{1}{2}|\Pr[A'(1,1) = 1] - \Pr[A'(0,0) = 1]| \\
&\qquad -\frac{1}{2}|\Pr[A'(1,0) = 1] - \Pr[A'(0,1) = 1]|
\end{aligned}
$$

Let A(b) be the outputs of A when the challenge is b.

$$
\begin{aligned}
&|\Pr[A(1) = 1] - \Pr[A(0) = 1]| \\
&\quad = |\frac{1}{2}(\Pr[A'(0,1) = 1] + \Pr[A'(1,1) = 1]) \\
&\qquad - \frac{1}{2}(\Pr[A'(0,0) = 1] + \Pr[A'(1,0) = 1])| \\
&\quad \geq \frac{1}{2}|\Pr[A'(1,1) = 1] - \Pr[A'(0,0) = 1]| \\
&\qquad - \frac{1}{2}|\Pr[A'(1,0) = 1] - \Pr[A'(0,1) = 1]| \\
&\quad \geq (\delta(n) - \mathrm{neg}(n))/2
\end{aligned}
$$

Public-key CCA2

- Is Construction **??** CCA2 secure?

Public-key CCA2

- Is Construction **??** CCA2 secure?
- **Problem:** Soundness might not hold with respect to the simulated CRS, after seeing a proof for an *invalid* statement

Public-key CCA2

- Is Construction **??** CCA2 secure?
- **Problem:** Soundness might not hold with respect to the simulated CRS, after seeing a proof for an *invalid* statement
- **Solution:** use *simulation sound* NIZK